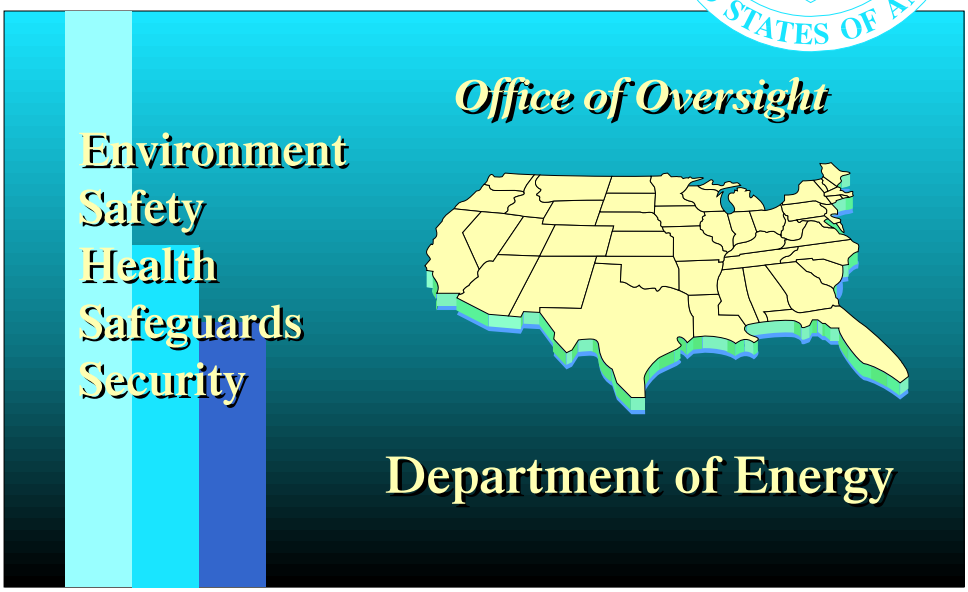
EH2PUB/07-97/08SE

OVERSIGHT

Portsmouth Gaseous Diffusion Plant

Safeguards and Security Profile Summary Analysis

July 1997



Office of Environment, Safety and Health

1.0 Introduction

The Department of Energy (DOE), Office of Environment, Safety and Health, conducted a review in July 1997 of the current safeguards and security posture at the Portsmouth Gaseous Diffusion Plant located in southern Ohio. The review was part of a recent initiative to characterize the current status of safeguards and security programs throughout the Department. The results of the review reflect the perspective of the Assistant Secretary for Environment, Safety and Health who, using the Office of Oversight, provides the Secretary of Energy with independent assessments of the Department's performance in the areas of environmental protection, safety, health, and security. This summary describes significant aspects of the safeguards and security posture at the Portsmouth Gaseous Diffusion Plant observed during this review.

2.0 Background

Location

The Portsmouth Gaseous Diffusion Plant occupies 3,700 acres of government property in south-central Ohio, approximately 120 miles east of Cincinnati and about 90 miles south of Columbus.

Mission

DOE's current mission for the Plant is to complete the high enriched uranium refeed/suspension, environmental restoration, and waste management programs. Additionally, the mission of the United States Enrichment Corporation, also located at the Plant site, is to produce low-enriched uranium for commercial nuclear power plants.

Security Assets/ Interests

The Plant possesses approximately 18,000 kilograms of high-enriched uranium items in the form of uranium hexafluoride, uranium oxides, and uranium scrap. Classified holdings consist of 134 documents, 5,000 to 6,000 (non-nuclear) parts, and about 100 personal computers and terminals that process classified information.

The Portsmouth Plant has a unique position within the DOE in that most of its facilities and activities have been assigned to the United States Enrichment Corporation; these activities are regulated by the Nuclear Regulatory Commission. However, significant quantities of DOE's high-enriched uranium are stored on site, and DOE continues to be responsible for security of this material until it is transferred off site or is "blended down" to lower enrichment (i.e., less

than 20 percent) so that it no longer requires the higher degree of protection afforded to high-enriched uranium. DOE plans to steadily remove or blend down the remaining high-enriched uranium within the next two years. This will gradually reduce the Department's security interests, and the Nuclear Regulatory Commission will assume sole responsibility for the site assets. In the interim, both the Nuclear Regulatory Commission and DOE have responsibilities for security interests under their respective purviews. Further, the Nuclear Regulatory Commission and DOE must coordinate to ensure that security systems that protect both DOE and Nuclear Regulatory Commission interests (e.g., alarm processing and monitoring equipment and computer networks) are appropriately inspected.

Protection Strategy

The Portsmouth Gaseous Diffusion Plant site employs a multiple-layered or "defense in depth" protection strategy. Defense in depth refers to multiple barriers – physical, electronic, and human – that form concentric circles of protection to provide a shield around the site's most valuable assets. Defense in depth protects against a broad range of adversaries, from a disgruntled employee to a highly motivated, trained, and skilled group of adversaries. In this protection strategy, the layers of defense include (1) physical barriers (fences, barbed wire, razor ribbon) and electronic intrusion detection systems at the exterior boundaries of the site; (2) the buildings in which the assets are located and the intrusion detection systems, alarms, access controls (described below), and search procedures also associated with those buildings; and (3) the vaults, vault-type rooms, safes and associated intrusion detection systems and administrative controls (see below) within the buildings in which the assets are stored.

Several administrative and electronic or mechanical protection measures are employed at various points throughout the layered boundaries. Administrative measures include the security clearances granted to personnel having access to the Plant's assets; a staff badging system for identifying cleared versus non-cleared staff; visual recognition and verification; numerous manned entry/exit points; various human reliability programs, such as personnel security assurance programs that employ random drug and alcohol tests and psychological testing for personnel directly accessing special nuclear material; and protocols such as "two person" rules, which assure that at least two personnel are present when nuclear material is being handled. Electronic/mechanical protection measures include various access controls, such as cipher locks, magnetic key cards and personal identification numbers, closed circuit television (for assessment), and an array of lock and key controls.

Finally, the Plant has a trained protective force to assess and respond to security matters anywhere within the multiple layers of the protection scheme described. While the site has no formal protective force special response team, it has kept the capability of one by retaining the special weapons and equipment previously held by that team, as well as by providing continued advanced tactical training to selected protective force members.

3.0 Results of Past Safeguards and Security Reviews

The last safeguards and security review by the Office of Security Evaluations revealed a generally effective protective force program, having only minor deficiencies in entry/exit search procedures. The concerns in the physical security systems program were the aging detection/alarm systems and a small number of various isolated deficiencies. Personnel security was deemed satisfactory, and material control and accountability had only minor issues noted in material accounting and equipment calibration practices. In protection of classified information, discrepancies were observed in document accountability records and in document destruction and courier practices. Finally, the computer security program displayed minor problems in password assignment and contingency planning.

4.0 Results of This Review

Positive Trends and Initiatives

The Portsmouth Gaseous Diffusion Plant has developed comprehensive plans for the disposition of all high-enriched uranium in its inventory according to its assigned DOE mission. At present, disposition efforts are ahead of schedule.

The safeguards and security program elements at the Plant are providing adequate protection for special nuclear material. The detection, delay, assessment, response, and administrative control elements of the program are designed and implemented to function in a complementary manner to provide the defense in depth required for the high-enriched uranium assets.

The Plant's computer security program demonstrates strengths that indicate unusually strong protection features. Classified computer security practices go beyond minimal requirements by incorporating procedures that physically disconnect computers from the classified local area network when the computers are not engaged in on-line sessions. In performance testing of the unclassified local area network, the barrier (firewall) used to prevent unauthorized access (penetration) into the network from outside sources was found to function effectively, successfully thwarting all penetration attempts.

Safeguards and Security Concerns

Challenges to Plant Management

Currently, as DOE security interests at the Portsmouth Gaseous Diffusion Plant recede and/or are turned over to the Nuclear Regulatory Commission, diligence will be required to ensure that the safeguards and security program

responds to changes in the site operational environment without allowing degradation of the protection provided to DOE security assets.

The DOE operations office (Oak Ridge) must continue to ensure that all safeguards and security program elements that affect the protection of DOE's assets, regardless of whether program responsibilities have been transferred to the Nuclear Regulatory Commission, are effective. For example, some computer security programs recently transferred to the United States Enrichment Corporation and which now fall under Nuclear Regulatory Commission regulation still provide protection for DOE classified information. However, Oak Ridge does not currently exercise any management or oversight responsibilities for the computer security programs at the Plant to ensure that DOE's classified information is adequately protected.

Accountability of Special Nuclear Material Remaining in Processing Equipment

One DOE requirement for safeguarding special nuclear material is that its type, designated category, form, quantity, measurement "values," location and other pertinent information be formally recorded or, in more specific terms, placed in material accountability records. The Plant is generally diligent in complying with this requirement. However, at one location on site, information regarding measurement values for nuclear material remaining in unused, shutdown processing equipment had not been entered into accountability, and at another location the measurement value information was found to be inaccurate, not having been adjusted based on recent measurements. Bringing all such information into accurate accountability would help reduce the Plant's cumulative historical nuclear material inventory differences.

Physical Security System Safeguards

As a prudent safeguards and security measure, it is advisable that the detailed knowledge of, and unlimited access to, certain critical security systems *not* be held by a sole individual. Allowing a single individual such access provides questionable assurance that the individual is not in some way altering, sabotaging, or otherwise subverting such systems. At the Plant, a single staff member on site possesses an in-depth knowledge of and unsupervised access to computer software used to control some of the Plant's security systems. Should those systems be purposely subverted, serious consequences could result. Although that person is enrolled in the Plant's personnel security assurance program, thereby providing some additional confidence in his trustworthiness, there is no direct observation or oversight of his actions.

Issues Warranting Management Attention

Access Credentials

Various formats are used for access credentials (badges) at the Plant. Over 50 badge types are used for visual site access identification, which could cause confusion and introduces the possibility of error by access control personnel and other employees when trying to ascertain an individual's authorization.

Computer Security Support

Although senior management is supportive of the Plant's classified computer security program, it has significantly decreased the availability of computer support personnel. Additionally, although the computer security site manager has strong management and technical skills, he is not receiving training to keep abreast of emerging technology. Further, he is performing computer security functions formerly shared among nine other individuals.